KPMG

Data Privacy matters

Local & Global Data Protection developments:

September 2021 – January 2022

Latest news in Data Privacy

March 2022

Contents

1. Executive Summary

Tom Hyland
Director

Risk and Regulatory Consulting
KPMG Ireland

Welcome to the first edition of our new Data Privacy Quarterly update, which outlines the most relevant developments and regulatory updates within the Privacy World.

The unexpected shift to working from home due to the COVID-19 pandemic has created new privacy and information security risks for organisations. Remote working has created its own risks, with employees working in potentially insecure environments, using new technology and they may be unable to react quickly to security incidents. While Privacy risks have been in the background of cybersecurity concerns, companies are now becoming more aware of the connectivity between business processes, third party processors and the enhanced privacy and information security risks.

The following are some recent developments:

- The Data Protection Commission ("DPC") in Ireland has published information regarding COVID-19 vaccinations and the privacy implications which surround that.
- The DPC has announced a new strategy covering the period from 2022 – 2027 and there will be changes to how breaches are reported.
- The Irish Government published the National Digital Strategy.
- Organisations have been given further clarity regarding the requirement to update contracts to include new Standard Contractual Clauses ("SCCs") in line with the Schrems II decision.
- The UK government has announced a new Online Safety Bill, while in Ireland an Online Safety and Media Regulation Bill has been published.
- ePrivacy remains at the top of regulatory agendas with new guidance on Cookies from Luxembourg and a new European Data Protection Board taskforce has been established to monitor cookie compliance across the EU.
- China's Personal Data Protection Law came into affect.
- US's Federal Trade Commission ("FTC") has announced new rules to protect Personal Data.

We hope you enjoy reading the newsletter, which contains further details on the matters above.

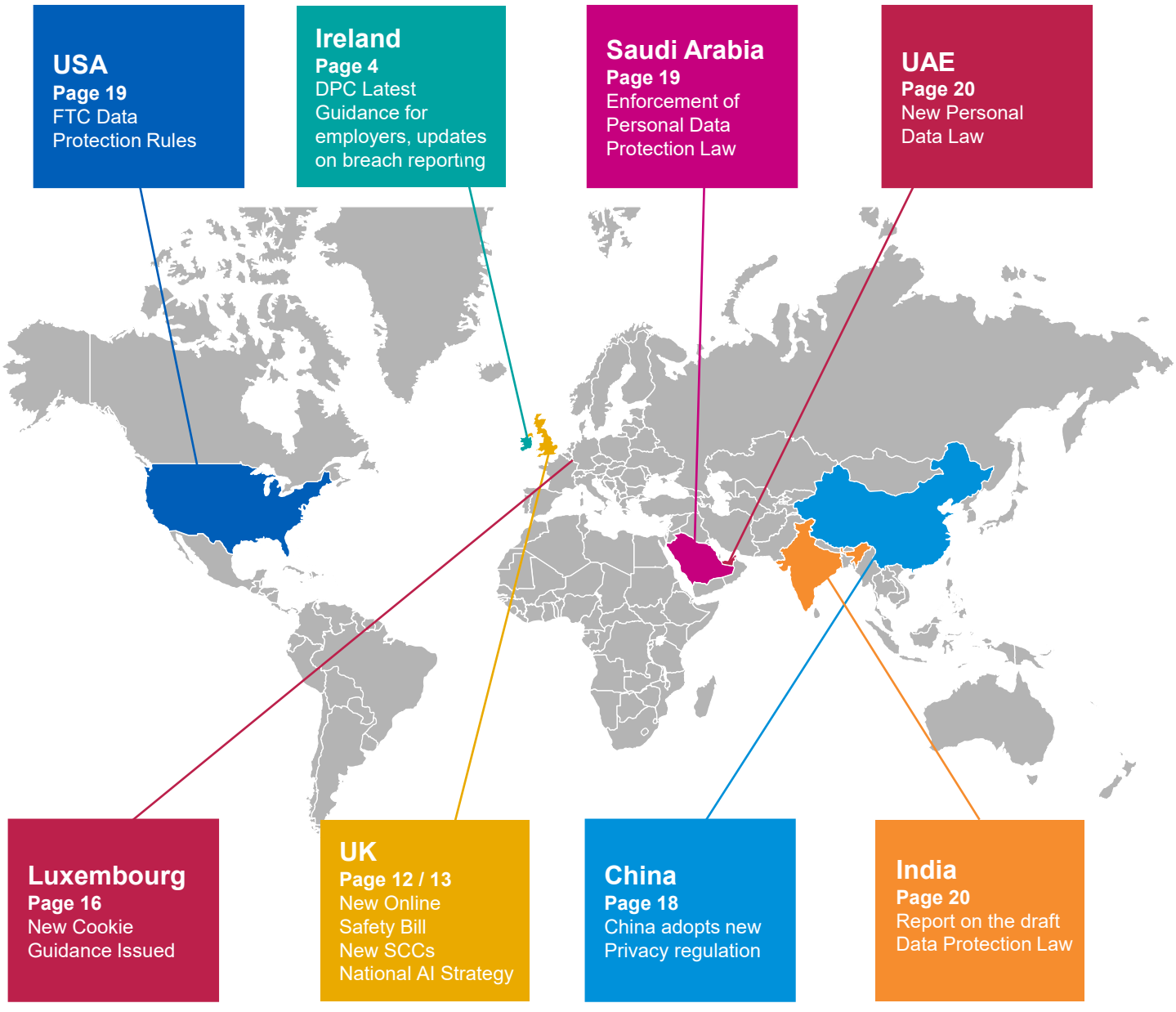
2. Regulatory changes across the Globe

Keeping up to date with the Privacy World

Data Privacy regulations are rapidly evolving. When implemented in May 2018, the General Data Protection Regulation ("GDPR") marked the beginning of global privacy regulations. However, new and emerging regulations in China, USA, United Arab Emirates ("UAE") and other countries have further changed the regulatory global landscape in relation to Data Privacy and in the digital world.

Organisations should take a proactive approach to data privacy which should evolve in line with new regulations and emerging technologies to empower your business. Your data privacy programme can create value and support privacy compliance and risk management while meeting the expectations of your customers, employees and vendors.

The diagram below is a snapshot of key privacy developments across the world.



3. Ireland

3. Ireland

Data Protection Commission ('DPC') Highlights

Updates from Ireland's Supervisory Authority

The DPC publishes Fundamentals for a Child-Oriented approach to Processing Data

In November 2021, the DPC released submissions to its public consultation on draft guidance in relation to appropriate children's data processing. Based on the feedback received, the DPC made some amendments to the guidance.

The Fundamentals introduced child-specific data protection interpretative principles and recommended measures that will enhance the level of protection afforded to children against the data processing risks posed to them by their access to services in both an online and offline world. The Fundamentals will also assist organisations by clarifying the principles arising from their high-level obligations under the GDPR.

The DPC has stated that its approach is not solely intended for organisations that have children as their target audience but also to those organisations whose services may be frequently accessed by children, even when this group is not their target audience. To comply with the principle of accountability, organisations must determine if they are collecting children's personal data and, if they are, they need to establish appropriate safeguards. Offline, this applies to educational providers, sports and social clubs, and health and social support providers amongst others. In a digital context, this includes websites, apps and other internet-of-things services which provide social media, media sharing, gaming, entertainment, educational, advocacy, health and social care/ support services.

The 14 Fundamentals are:

- Floor of protection. Online service providers should provide a "floor" of protection for all users, unless they take a risk-based approach to verifying the age of their users.
- Clear-Cut Consent. Consent should be freely given, specific, informed and clear.
- Zero Interference. Organisations should ensure that legitimate interests do not interfere with the best interest of the child.
- Know your Audience. Organisations should take steps to identify users to ensure that children are protected.
- Information in every Instance. Organisations must be transparent by offering the information about the processing of their data to children.
- Child-Oriented Transparency. Information must be given in an intelligible and accessible way
- Let Children Have Their Say. Children may exercise their data subject rights at any time.
- Consent does not change childhood. Children cannot be treated as adults just because consent is obtained.
- Your Platform, Your Responsibility. Prove that the measures around age and verification of parental consent are effective.
- Do not Downgrade Children's Experience. Children cannot be deprived of a rich service experience to avoid these obligations.
- Minimum User Ages are not an excuse. User ages thresholds do not provide a free pass to not comply with these obligations.
- A precautionary approach to Profiling. If an organisation profiles children, it needs to demonstrate how it is in the child's best interest.
- Do a Data Protection Impact Assessment (DPIA). Online service providers should undertake DPIAs, the child's best interest should be a key criterion.
- Bake it In. Data protection measures should be built into the architecture and functioning of a product from the very start of the design process.

It is worth noting that the DPC took into account the "Age Appropriate Design Code" issued by the ICO when drafting the Fundamentals. The DPC is focused on creating a safer space for children, this aligns with their strategy for the next five years as one of its strategic goals is to "Prioritise the protection of children and vulnerable groups". The Fundamentals have immediate effect so data controllers are expected to be compliant as there will be no implementation period. Furthermore, the DPC clarified that the Fundamentals are not a statutory code.

Organisations must assess their operations, processes, systems and controls to ensure that they comply with the Fundamentals and they can demonstrate that their practices have the child's best interest at heart.

The Fundamentals can be found here.

Data Protection Commission ('DPC') Highlights

Updates from Ireland's Supervisory Authority

The DPC publishes guidance on vaccination checks.

In November, the DPC published guidance on vaccine certification checks for data controllers and data subjects.

In the Guidance, businesses are identified as data controllers, as such, they are required to identify the legal basis to ask for and verify the vaccination status of individuals that access their business premises.

They cannot retain any personal data after vaccine verification and are subject to the EU General Data Protection Regulation. The DPC establishes that businesses will be able to rely on public interest purposes in the area of public health, however the necessity will need to be assessed based on up-to date advice.

In addition, businesses can also rely on the fact that they have a legal obligation set out in-the Health Act 1947 (Sections 31AB and 31AD) (COVID-19) (Operation of certain indoor premises) Regulations 2021.

Finally, the DPC established that:

- The information cannot be retained.
- The business do not have to carry out a Data Protection Impact Assessment (DPIA) as the scope of the processing is limited and based upon public health requirements.
- The business cannot use the personal data for any further processing.

As the public health advice has changed quite recently, it is expected that these guidelines will be updated accordingly.

The DPC completes the Data Protection Officer enforcement programme

The DPC has completed the most recent stage in its Data Protection Officer enforcement programme aimed at improving compliance with Article 37 of the GDPR.

The programme, which was initiated in 2020, assessed the compliance of public bodies with their obligations under Article 37.7 of the GDPR (requiring public bodies to appoint DPOs). The DPC has identified 77 potentially non-compliant public bodies from a total number of 250. Following this inspection, 70 organisations brought themselves to be compliant.

This year, the DPC expanded the programme to include the private sector, even though there is no automatic requirement for non-public sector organisations to appoint a DPO. The DPC has identified several sectors likely to meet the threshold to appoint a DPO, including private hospitals and out of hours GP services, banking entities, and credit unions. As a result of the DPC's inspection the number of compliant entities within the country has increased.

Before extending compliance checks to other sectors, the DPC will consider whether further guidance is necessary to address any issues of concern.

Organisations must assess the nature of their processing activities, as a DPO must be appointed if they meet the scale and nature threshold set out by the DPC. In addition, the DPC will continue to monitor organisations that were under the scope of this initial review to identify whether they are compliant with Article 37(1).

A full summary of the DPC findings is available here.

The DPC publishes its Regulatory Strategy for 2022-2027

The DPC has published its strategy for 2022-2027. The DPC believes that these will be crucial years in the evolution of data protection law, regulation and culture. The strategy is structured according to the DPC's fundamental goals which are underpinned by the DPC's mission, vision and values. The strategic goals are as follows:

- Regulate consistently and effectively;
- Safeguard individuals and promote data protection awareness;
- Prioritise the protection of children and other vulnerable groups;
- Bring clarity to stakeholders; and
- Support organisations and drive compliance.

One overarching objective - to do more, for more – has underpinned the strategic choices made in this strategy, as the DPC navigates a regulatory future replete with competing priorities.

More information can be found here.

3. Ireland

The DPC is changing how it handles data breach reports

The Deputy Commissioner has announced substantial policy changes in how the DPC will deal with breach notifications going forward. The DPC has put in place a new form for breach reporting. Speaking at the 16th Annual Data Protection Compliance Conference, a DPC representative stated that there will no longer be immediate engagement from the DPC, and it will no longer offer guidance on mitigation. The DPC will continue to investigate and determine whether a statutory inquiry is needed. In addition, it was stated that the DPC is going to be stricter with controllers that fail to acknowledge requests from data subjects.

Summary of Key Changes

Section 1 - Introductory questions

Users will be required to confirm whether the breach is likely to result in a risk to the rights and freedoms of natural persons and whether the breach falls under the Law Enforcement Directive.

Section 2 – Your Supervisory Authority

The new published form will guide users to determine whether the breach relates to cross-border processing. In addition, the user will have to answer questions including details of the controller's establishments, location of affected data subjects and whether they are "substantially affected", as well as the nature of the DPC's competence in relation to the subject matter of the breach notification.

Section 3 – About You

Controllers will have to specify the industry sub-sector according to Eurostat NACE criteria. In addition, controllers will also have to specify whether the notifying person or the DPO is the main point of contact for the breach notification.

Section 5 – Details of the Breach

The DPC has included more detailed options in relation to the nature of the breach and for the types of data affected by the breach.

Section 6 – About the Data Subjects

The new form will require the controllers to choose the approximate numbers from a range of bands (1-10, 11-100,…) rather than include a specific number.

Section 7 – Action Taken

The new form requires users to include additional details of technical and organisational security measures including:

- Measures in place prior to the breach occurring;
- Deficiencies identified;
- Measures taken or to be taken to mitigate the impact of the breach on affected data subjects; and
- Measures put in place in order to reduce the likelihood of re-occurrence.

Section 8 - Communication to affected data subjects

If the controller has used a public communication to inform affected data subjects of the breach, the new form requires the controller to explain why it would have involved disproportionate effort to notify data subjects individually.

Here you can know more about the changes on data breach reporting. Link to the data breach form here.

3. Ireland

Ireland Online Safety Bill

The Online Safety and Media Regulation Bill has been put forward to align with the new era of accountability in online safety. It moves towards a holistic approach to the regulation of online services, and reduces the availability of harmful content online.

Media Commission

A key part of the Bill is that it establishes a new regulator to ensure accountability in the sector.

The Irish government plans that the Broadcasting Commission of Ireland will eventually be subsumed into a new regulator, the Media Commission (Coimisiún na Meán). The new regulator will include an Online Safety Commissioner to enforce the Online Safety and Media Regulation Bill and additional forthcoming legislation, including at an EU level. The Commission will form a vital part of a new network of digital regulators both across the EU and in Ireland, including the Data Protection Commission and the proposed Gambling regulator.

Online Safety Bill

This Bill is a first in regulating harmful online content. This includes content that is deemed illegal under a number of specific Irish criminal law statutes as well as specific categories of harmful content which meet a certain risk threshold including bullying, and the promotion of self-harm or suicide.

The potential range of regulated service providers is significant. Any online service that facilitates user-generated content could be in scope meaning that private messaging and online storage services are potentially in scope.

It is unlikely that all aspects of harmful online content can be addressed in this Bill. However, it is expected that there will be regulation coming from the EU and the Irish government.

Impact for organisations

It is crucial that organisations remain vigilant and aware of their obligations ahead of upcoming changes to regulation. If in scope organisations fail to comply with the new online safety codes, subject to court approval, the new Commission will have the power to sanction non-compliant online services. This includes financial sanctions which are on par with the GDPR enforcement fines.

3. Ireland

Harnessing Digital - The Digital Ireland Framework

The Irish Government published the new National Digital Strategy presenting a list of objectives for 2030. This Strategy is a high-level framework to support Ireland's ambition to be a digital leader. The Digital Ireland Framework is in line with the EU's target of digital transformation for 2030.

The list of goals that have been set can be classified in four areas: digital transformation of business, an improvement to digital skills, development of digital infrastructure and the digitisation of public services. The main targets of the Government are:

- Making connectivity available to everyone
- Providing digital skills to the population
- Build inclusive digital public services
- Digitise Irish businesses
- Invest in cybersecurity
- Implement a well-resourced regulatory framework

Under the new digital strategy, Ireland will nominate a regulator to act as Ireland's digital services co-ordinator under the EU's recently approved Digital Services Act.

The DPC welcomed the publication of the National Digital Strategy stating that effective and appropriate regulation will be key to achieve the goals set by the Government. You can read the statement here and more about 'Harnessing Digital - The Digital Ireland Framework' here.

4. European Union and the UK

European Union News

AML Action Plan

The European Data Protection Supervisor ('EDPS') has come out in support of the European Commission's proposed Anti-Money Laundering legislative package and suggested improvements regarding the protection of personal data. It was stated that intrusion into individuals' privacy must be minimised despite the proposal taking a risk-based approach to assessing whether individuals present a money-laundering risk. The recommendations from a data protection perspective include categories of personal data that may be processed, and clearer definition of roles in respect of those involved in the supervision model. The EDPS also recommended adding an express reference to the protection of personal data to the list of risks to be considered by member states.

Read more on the EDPS opinion here.

European Union Data Governance Act

The Data Governance Act ('DGA') will set up robust mechanisms to provide a framework for sharing industrial data across the EU, facilitate the reuse of certain categories of protected public-sector data, increase trust in data intermediation services, and foster data altruism across the EU.

The Data Governance Act will apply to the following situations:

- The Act will allow public sector data to be made available for re-use in particular situations;
- The Act will allow the sharing of data between organisations;
- The Act will allow personal data to be used through data intermediation services, through whom data subjects could make their data available to potential users of the data using a secure environment; and
- The Act will allow individuals and companies to share or make data available on a voluntary basis for the common good.

The Irish Government announced in December 2021 that the establishment of the Data Governance Board had been completed.

The European Data Protection Board had expressed concern regarding the data privacy implications of the proposed new regulation.

The European Council have provided information here.

4. European Union and the UK

The GDPR under review

The EDPS has proposed a June 2022 review of the effectiveness of EU General Data Protection Regulation enforcement.

The EDPS stated that it was uncertain whether the GDPR needed to change or not but that a review was needed to ensure that the regulation adequately addresses the constant technology changes and plan what the forecast should be in the prospect of five years and 10 years.

On 16 -17 June 2022, the EDPS will host the conference 'The future of data protection: effective enforcement in the digital world'.

Listen to the Digital Belief Podcast here.

Restrictions of data subject rights Guidelines Published

The European Data Protection Board adopted a final version of its guidelines on restrictions of data subject rights under the GDPR's Article 23, 'Restrictions'. The guidelines aim to recall the conditions surrounding the use of the Article 23 restrictions in light of the Charter of Fundamental Rights and the GDPR.

The guidelines provide an analysis of the criteria which can be leveraged to apply restrictions, the assessments that need to be observed, how data subjects can exercise their rights after the restrictions are lifted, and the consequences of infringements of Article 23 GDPR. Additionally, the guidelines analyse how the legislative measures setting out the restrictions need to meet the foreseeability requirement and examine the grounds for the restrictions listed by Art. 23(1) GDPR, and the obligations and rights which may be restricted.

The guidelines provide a definition for 'restrictions'
and note that restrictions must pass a necessity and proportionality test in order to be compliant with the GDPR, and that this test should be carried out before the legislator decides to provide for a restriction. This means that restrictions which are found to be extensive and intrusive cannot be justified.

The guidelines can be found here.

EUROPEAN DATA PROTECTION BOARD ('EDPB')

EU Adequacy decision for South Korea

On September 27th, the European Data Protection Board ('EDPB') adopted its opinion on the European Commission's draft adequacy decision for the Republic of Korea.

The EDPB also identified certain aspects of the Korean data protection framework that require further examination and clarification to ensure an equivalent level of protection:

- The exemptions under Korean Data Protection law when processing pseudonymised information.
- The adequacy decision will cover transfers from the Europe Economic Area ('EEA') to "processors" in Korea, however Korean authorities need to clarify if "personal information controllers" as described in the Personal Information Act (PIPA) will also be covered.
- Access by public authorities to data transferred to South Korea.
- The EDPB also asked to clarify the requirements to file a complaint with the Korean data protection authority, to ensure that individuals are provided with effective remedies and right of redress.

In December, the European Commission issued the adequacy decision. The exceptions are:

- Religious organisations (missionary activities);
- Political parties (nomination of candidates); and
- Controllers that are subject to oversight by the Financial Services Commission for the processing of personal credit information pursuant to the Credit Information Act, to the extent they process such information.

The EU Commission holds that South Korea ensures a level of protection for personal data transferred that is "essentially equivalent" to the one guaranteed by the GDPR. Considering further findings, the Republic of Korea would ensure an "adequate level of protection" within the meaning of Art. 45 GDPR.

You can find the opinion here and the adequacy decision here.

4. European Union and the UK

Guidelines on the interplay between article 3 and international transfers

In November 2021, the European Data Protection Board ('EDPB') published its Draft Guidelines 05/2021 on the Interplay between the application of Article 3 GDPR and the provisions on international transfers as per Chapter V of the GDPR, which was open for public consultation until 31 January 2022.

According to the EDPB's press release, the Guidelines aim to assist controllers and processors in the EU in identifying whether a processing operation constitutes an international transfer, and to provide a common understanding of the concept of international transfers.

The Guidelines specify three cumulative criteria that qualify processing as a transfer:

- The data exporter (a controller or processor) is subject to the GDPR for the given processing;
- The data exporter transmits or makes available the personal data to the data importer (another controller, joint controller or processor); and
- The data importer is in a third country or is an international organisation.

The processing will be considered a transfer, regardless of whether the importer established in a third country is already subject to the GDPR under Art. 3 GDPR. However, the EDPB considers that collection of data directly from data subjects in the EU at their own initiative does not constitute a transfer.

The European Commission confirmed that it will develop a new set of SCCs for transfers under article 3(2) of the GDPR once the EDPB publishes the final version of the Guidelines. The new SCCs will coexist with the current SCCs.

You can find the Guidelines here.

4. European Union and the UK

The European Commission (EC) reviews the EU-Japan Adequacy Agreement

In October 2021, the Personal Information Protection Commission of Japan (PPC), the European Commission, and other data protection authorities started the first review of the EU-Japan mutual adequacy agreement adopted in 2019.

According to the press release, the review covers all aspects of the functioning of the adequacy decisions adopted by the EU and Japan, from their application to broader legal developments in the areas of data protection and government access to data. It offers also an opportunity to share information and experience on issues of common interest.

The European Commission and PPC will publish separate reports on the functioning of their respective adequacy decisions. These reports will conclude the review process.

Here you can find the press release.

UK New SCCs – ICO Consultation

In October 2021, the consultation opened by the Information Commissioner's Office ('ICO') about the equivalent instrument to the SCCs in the UK was closed.

The "international data transfer agreement" is the UK's version of standard contractual clauses (SCCs). The ICO chose to depart from the wording in the UK GDPR which refers to "standard data protection clauses" and the commonly used term "standard contractual clauses" was not specified in the consultation but it seems that is intended to make the term more understandable to those less familiar with the legislation.

The ICO published, on 31 January 2022, its statement in response to the Department for Culture, Media and Sport ('DCMS') laying, on 28 January 2022, the International Data Transfer Agreement ('IDTA'), the International Data Transfer Addendum to the European Commission's Standard Contractual Clauses ('SCCs'), and a document setting out transitional provisions as to the use of the current SCCs for international data transfers before Parliament. The ICO noted that the IDTA, Addendum, and transitional provisions will now lay before Parliament until they come into force on 21 March 2022. Organizations may continue to use the EU SCCs as a valid transfer mechanism for transferring personal data from the UK under new contracts until 21 September 2022. You can read the statement here

4. European Union and the UK

UK National Artificial Intelligence Strategy

In September 2021, the UK Government announced its National Artificial Intelligence Strategy ('NAIS') for the next 10 years. This strategy is based on several assumptions about what will happen in the Artificial Intelligence ('AI') scene in the next decade. The first one being that for AI to thrive, it needs to have access to four key elements: people, data, computing power and finance. The second assumption is that AI will eventually become ordinary, so it will be part of the economy and most sectors and industries will avail of AI. Lastly, regulation needs to adapt to AI to ensure that it encourages innovation, but it also protects the security and freedom of citizens.

Based on these three assumptions, the agencies involved set key actions over the next 12 months and beyond, focusing on investment and planning for long-term needs, transitioning to an AI-enabled economy, and encouraging innovation and investment through governance of AI technologies.

In the short term, the government aims to publish a framework to set the government's role in increasing data availability. In addition, it will open a consultation on copyright and patents, and it will also clarify the role of data protection in AI Governance.

In the medium term, the UK will create new visa programmes to attract more talent into the AI economy as well as creating new aid programmes to encourage innovation in developing countries. It is also worth noting that the UK plans to create an AI standards hub to work on the coordination of global AI standardisation.

In conclusion, the UK wants to become an "AI superpower" by identifying the AI factors that can help create new economic opportunities. However, it remains to be seen how the government will support the commercial AI sector that is already in place, as well as some key definitions such as what it is considered AI and what it is not. In the following months, monitoring the developments of the short-term activities might be able to help answer some key questions, specially the most important one which is how AI could be leveraged to create and drive economic growth and productivity and how to encourage the public to trust AI.

For more details on the plan please check the government website.

UK Online Safety Bill

Background

In May 2021, the UK government published the initial draft of the Online Safety Bill. This Bill aims to address illegal and harmful content online for children and adults.

Scope

The providers of regulated services that will be under the scope of the new regulation will be, specifically:

- User-to-user services: Internet services that allow users to upload, generate, or share user-generated content or otherwise to interact online with other users, i.e., social media platforms such as TikTok or Instagram, online marketplaces like Wallapop, and online forums such as Reddit.
- Search services: Services that allow users to search all or some parts of the internet such as Google.

The regulation is extra-territorial and will apply to regulated services with links to the UK. A provider will be considered to have links to the UK if it has a “significant” number of users in the UK, however significant has not been defined yet, or if the content of the platform is being targeted towards UK users; or if the provider can be used by individuals in the UK; and there is a material risk of significant harm to individuals in the UK arising from content on/via the service provided.

Nevertheless, the Bill outlines several exemptions, outlined in schedule 1 of the draft.

Relevant content

According to the draft, companies will be divided into categories. These categories will be based on the number of people using the providers’ online services. The Secretary of State will make secondary regulations to determine the threshold conditions of each category.

Large social media sites that pose a higher risk to users are likely to be classed as “Category 1” organisations and will have more obligations to moderate content. “Category 2” organisations will be divided into two subcategories (2A and 2B). Any interactive community platform that promotes the sharing of user-generated content, such as travel sites, online gaming, dating or private messaging are likely to be included in any of these subcategories. This means that most companies will be classified in the Category 2 as they will be deemed low risk, however they will still be required to act against illegal and harmful content.

Providers will be expected to comply with a series of duties aiming to reduce the presence of content that promotes terrorism, child sexual abuse and, in general, any type of abuse content. In addition, the Bill aims to minimise the time that it takes for such platforms to remove the content once it is spotted as well as address the risk of children accessing harmful content. The government has confirmed that companies will have a duty of care towards the platform users.

Finally, if the Bill is introduced into law in its current form without further amendments, companies will also have a duty towards safeguarding free speech and privacy rights. Providers will also have to ensure that they have sufficient measures in place to protect journalistic content and content of “democratic importance”.

Legal but harmful

Defining "legal but harmful" material seems to be one of the key challenges. In the draft, harmful content is defined as content that the provider has “reasonable grounds to believe” gives rise to a “material risk” of a “significant adverse physical or psychological impact” on an adult or child “of ordinary sensibilities”. Secondary legislation will define “harmful content” to provide further clarity. The expectation that providers will have to look out for content that is not unlawful but that falls within the definition means that providers will be liable for content that will not create any liability for the user that publishes it.

Enforcement and Secondary Regulation

According to the draft, Ofcom will become the online safety regulator.

A super-complaints procedure will allow certain eligible entities to make a complaint to Ofcom (eligible entities have not been defined yet, however additional regulations are expected). It is worth noting that the Bill does not introduce new routes for individuals to bring claims directly against providers.

What’s next

In December 2021, the report on the draft bill was published outlining several recommendations such as providing more clarity around what is illegal online content and to add an obligation for service providers to record additional threats to safety including “the potential harmful impact of algorithms”. The Government has a two-month window to respond to the Committee’s recommendations.

DORA

The EU's Digital Operational Resilience Act for financial services

What is DORA and why now?

DORA aims to regulate how to address Information and Communication Technology ('ICT') risks in a consistent way to avoid the disparities between addressing digital risks and building operational resilience which have been seen in every Member State. DORA will establish an ICT Risk Management Standard in Europe. At the same time, this regulation will complement the GDPR and the Information Security Directive. The final regulation is expected to be published this year and set to be agreed before summer 2022.

The DORA aims to:

- Strengthen the overall identification, mitigation and management of ICT risks and thus the overall effectiveness of the firm's preventive and resilience measures while equally being proactive to identify and remedy vulnerabilities;
- Eliminate redundancies and barriers that hinder the efficient reporting of ICT-related incidents;
- Increase supervisors' threat knowledge and incident awareness;
- Develop and deploy more resilient testing frameworks; and
- Increase the oversight and monitoring by firms of the risks and resilience measures employed by third-party ICT providers to better manage risks including on over-dependence on such firms.

Who is under the scope of DORA?

The DORA not only covers financial firms across every sector of the finance industry, it also applies to third party providers such as cloud services that are suppliers to financial institutions. This means that DORA brings 'critical ICTs third party providers' within the regulatory perimeter.

Each critical ICT third-party service provider must assess whether they have comprehensive and effective rules, procedures, mechanisms and arrangements in place to manage the ICT risks that it may pose to financial entities, as this will be a requirement from the financial institutions in order to keep them as providers (such as rapid reporting of cybersecurity incidents, ability to respond rapidly to audit requests from the regulators and offer access to the premises).

What does the DORA require of financial entities and ICT providers?

DORA introduces requirements across a number of pillars: ICT Risk Management, ICT-related Incidents Management, Classification and Reporting, Digital Operational Resilience Testing, ICT Third-Party Risk Management, Information and Intelligence Sharing. The following are key requirements:

- To have internal governance and control frameworks that ensure an effective management of all ICT risks.
- The DORA will set clear roles and responsibilities for all ICT-related functions, determine the appropriate risk tolerance level of the financial entity's ICT risk and agree the financial entity's policy on arrangements regarding the use of ICT services provided by third-party service providers.
- Financial entities would have to validate third-party providers to ensure that they only enter into contractual arrangements with ICT third-party service providers that comply with the latest information standards. The same applies to sub-contracting arrangements, especially when an ICT third-party service provider is established in a third-country.

What should financial entities and ICT providers do to prepare for the DORA?

Implement, maintain and periodically update:

- ICT risk management frameworks;
- ICT systems, protocols and tools that are reliable and technologically resilient to deal with additional information processing needs;
- Identify, classify and document all ICT-related business functions, identify on a continuous basis all sources of ICT risk, and assess cyber threats and ICT vulnerabilities;
- Carry out on-going monitoring and control the functioning of the ICT systems and tools and minimize the impact of risks through the use of ICT security tools, policies and procedures;
- Business continuity and IT disaster recovery policy as an integral part of their operational business continuity policy;
- Embed a back-up policy specifying the scope of the data that is subject to back-up and the minimum frequency of the back-up, and recovery methods;
- Carry out audits following significant ICT disruptions; and
- Implement ICT-related incident management processes.

EU Perspective: ePrivacy and Cookies

Upcoming ePrivacy Regulation

The ePrivacy Regulation is a set of data privacy laws first proposed in January 2017 which complement the GDPR and were intended go into effect alongside GDPR in 2018. The regulation provides rules on cookies and consent. The regulation puts accountability for obtaining consent to store cookies "on the entity that makes use of processing and storage capabilities of terminal equipment or collects information from end-users' terminal equipment, such as an information society service provider or ad network provider."

The European Parliament and the European Council have not landed on decisions for a number of significant issues such as the scope of the prohibition of direct marketing, the definition of 'unwanted calls' and 'direct marketing. It is not expected that the ePrivacy regulation will go into full effect for approximately 24 months.

The draft ePrivacy text can be found here.

Luxembourg publishes cookie guidance

Luxembourg's National Commission for Data Protection published updated guidelines on cookies and other trackers to help websites and applications comply with applicable rules. In the guidelines, the CNPD offers comment on essential and non-essential cookies, discusses the notion of dark patterns in the context of obtaining user consent and shares examples of good practice.

Information can be found on the Luxembourg Supervisory Authority here.

Cookie Banner scrutiny leads to the establishment of a new EDPB taskforce

In response to complaints concerning compliance of cookie banners to several supervisory authorities across the EEA, the EDPB has established a taskforce to coordinate the response to complaints. The organisation making the complaints is NOYB, a non-profit organisation founded by the privacy activist, Max Schrems, who is behind the Schrems case that led to the invalidation of the EU-U.S. Privacy Shield mechanisms for transfers of personal data to the U.S.

The EDPB taskforce is established in accordance with Art. 70(1)(u) of the GDPR, which states that the EDBP must promote the cooperation and effective bilateral and multilateral exchange of information and best practices between SAs. The taskforce will work to streamline communication between the authorities, exchange legal analysis and views on possible infringements, and provide support nationally.

What does this mean for organisations in the EU?

The EDPB is focusing more on the compliance of organisations in relation to their cookie banners, and likely their compliance with the ePrivacy Directive.

The EDPB has published details on this task force here.

5. International

China's Personal Information Protection Law comes into effect

On November 1st, China's new Personal Information Protection Law (PIPL) came into effect. The PIPL will work in conjunction with the Cybersecurity Law and the Data Security Law.

The PIPL not only applies to processors within the PRC, it also applies to the cross-border transmission of personal information and applies extraterritorially when the processing is happening outside of the PRC in the following scenarios: Providing a product or service to data subjects located within the PRC; Assessing the behaviour of individuals located within PRC or any other situation as described in Article 3 of the PIPL.

Changes in the legal basis of processing

The PIPL expands the legal basis of processing in the PRC as consent was the only legal basis to process personal data. The following legal bases have been included in addition to consent:

- Performance of a contract or necessity arising from the human resources management implemented in accordance with the labour rules and regulations of the employer formulated according to the law or collective contracts signed according to law.
- Compliance with legal obligations.
- Response to public health emergency or to protect the safety of individuals' health and property.
- Processing information that has been made public within "reasonable scope".
- To carry out new reporting and public opinion monitoring for public interests.

Obligations

The PIPL sets several obligations for entities that handle personal information:

- Appoint a DPO when the processed personal information exceeds a threshold. This threshold has not been established within the PIPL.
- Understand when a DPIA is required and put in place a process to conduct regular audits.
- Appoint a local representative that will be responsible for handling issues relating to personal information processing.
- Notify the authorities and the data subjects in the event of a data incident. It is worth noting that they must also notify the relevant parties if a data incident is "likely to occur".

Cross-border transfers

International transfers of personal information will only be allowed when there is a legitimate purpose such as a business need. The Processor will have to comply with one of the following requirements prior to exporting data:

- Completing a security assessment. Draft measures were issued in late November 2021 to offer guidance on how to complete these assessments. Organisation must complete these assessments when:
  - They transfer "important data";
  - Collect personal information of > 1 million people;
  - Transfer personal information of > 100,000 people; and
  - Transfer "sensitive" information of > 10,000 people.
- Undergoing a personal information protection certification.
- Entering into a contract with a foreign recipient.

As several concepts and obligations are still not clear within the PIPL, it is expected that secondary legislation and guidelines will be published. However, organisations are still expected to comply with the regulation from November 1st if they want to avoid being fined. It is also expected that this new law and any laws which are subsequently published will aim to tackle the challenges associated with new technologies, specifically anything related to Artificial Intelligence. Organisations with links to the PRC territory must keep monitoring further developments regarding secondary legislation and ensure their activities are compliant with the PIPL.

The (non-official) translation of the legislative text can be found here.

5. International

FTC implements tougher data protection rules to safeguard customer information

The US Federal Trade Commission ('FTC') has amended its data protection policy, implementing tougher rules for financial institutions that process customer information.

The agency's Standards for Safeguarding Customer Information has been changed under the Gramm-Leach-Bliley Act (GLBA). The GLBA provides a framework for regulating the privacy and data security practices of a broad range of financial institutions in the US, at a federal level (e.g. Institutions that fall under the scope of this act need to provide customers with information about their privacy practices and their opt-out rights).

This review is designed to address the significantly increased complexity of information security, and the chain of damaging data breaches that have plagued the financial services industry in recent years. Certain aspects of the amended rule – such as requiring written risk assessments, penetration testing and vulnerability assessments, and employee training – will take effect one year after the date of publication of the Standards in the Federal Register, while all other provisions will take effect 30 days after publication.

The key consideration of these amendments are:

- The term "financial institution" has been expanded to include those that engage in activities considered to be incidental to financial activities (e.g. companies that look for buyers of a product to introduce them to sellers will be now within its scope).
- Financial institutions must implement and maintain specified security controls to safeguard customer information (e.g. Encryption, multi-factor authentication).
- Customer information must be disposed of no later than two years after the last date the information is used in connection with providing a product or service to the customer.
- Financial institutions must conduct regular testing and monitoring of the effectiveness of their key data security controls, including continuous monitoring or periodic penetration testing and vulnerability assessments of applicable information systems.

The FTC will continue to scrutinise financial institutions to ensure that they are compliant with the new privacy requirements. All financial institutions that fall under the scope of this rule should take action to ensure that their privacy frameworks and security programs are up to standard. You can read the press release here.

Saudi Arabia: Personal Data Protection Law

Saudi Arabia's new Personal Data Protection Law has now been published in the Official Gazette. The Law will come into effect on 23 March 2022.

Entities with operations in Saudi Arabia or those processing data of Saudi residents will have one year to comply with the new requirements.

The supervisory authority, Saudi Data & Artificial Intelligence Authority ("SDAIA"), will implement regulations supplementing most aspects of the law by March 2022.

Key points to note are as follows:

- Data controllers must prepare and register data processing activities;
- Breach notification obligations;
- Further regulation of sensitive personal data, which includes genetic, health, and credit and financial data;
- Data controllers must register with SDAIA and pay an annual fee;
- Consent Management regulations;
- Restrictions on cross-border transfers;
- The law applies to the personal data of all Saudi residents; and
- The law applies to any entity processing data in the Kingdom or by entities located outside the Kingdom.

5. International

UAE's landmark new personal data laws

Summary

The United Arab Emirates has issued its first data protection law alongside a law establishing the new UAE Data Office. The law has extraterritorial effect and will apply to both controllers and processors that are located in the UAE and those located outside the UAE that process the personal data of individuals in the UAE.

Key Provisions

Legal Bases. The Data Protection Law prohibits the processing of personal data without the consent of the data subject, unless an exception applies.

Data subject rights. Data subjects will have a number of rights under the Data Protection Law with respect to their personal data: (i) the right to receive information from a controller; (ii) the right to request the transfer of their personal data; (iii) the right to have their personal data corrected or erased; (iv) the right to restrict the processing of personal data in certain cases; (v) the right to object to certain types of data processing; and (vi) the right to object to automated processing. Controllers are required to put in place a mechanism for communicating with data subjects. These rights are similar to the ones outline in the GDPR.

DPO. Companies will need to appoint a DPO under certain circumstances.

Data Breaches. Data breaches that are likely to result in a risk to the privacy, confidentiality and security of personal data must be notified to the UAE Data Office.

International transfers. Personal data may be transferred outside the UAE to states or territories that offer an adequate level of protection but subject to the approval of the UAE Data Office

The law has taken effect

The Data Protection Law is in effect as of 2 January 2022, although it is anticipated that further executive regulations will clarify various aspects (including the scope and level of sanctions). Controllers and processors will then have a period of six months from the date of issuance of such regulations to adjust their status and comply with the Data Protection Law.

India Data Protection Law: Proposed changes

In December 2021, the Joint Parliamentary Committee (JPC) of the Indian Parliament issued its report after almost two years of discussion.

The Reports brings India one step closer to have a final draft of the Data Protection Law.

Some of the highlights of this report are:

- Inclusion of Non-Personal Data within the Scope of the Law. The Data Protection Authority will govern personal and non-personal data.
- Data localisation. Where existing personal data is held by entities out of India, storing a copy of sensitive and critical data within India it is being required . It is reiterated that government surveillance over such data will be subject to strict application of the principle of necessity.
- The DPO should reside in India and be part of the "key managerial personnel" of the organisation.
- The report requires to modify the language of the draft provision to clarify that the data subject's consent must be obtained based on the context of the collection.
- Organisations working exclusively with children's data must register with the Data Protection Authority.
- Social Media platforms will be treated as "publishers" when they have control on the visibility and target audience of the content hosted on their sites. In addition, these organisations will need to have a physical office in India.
- Timelines for implementation. Organisations will have 24 months to implement all the provisions of the Act.
- Cross-border transfers. When approving a contract or intragroup scheme that allows the cross-border transfer of data the DPA should now consult the government prior to approval.

It is likely that 2022 will be the year that India sees its first general data protection law in place. The Indian Parliament might discuss this draft law in February 2022.

Read more about it here.

How KPMG can help

We are a leading provider of Data Privacy and Protection solutions in the Irish Market supported by a large Global team to support the needs of local and multinational organisations.

We have extensive Data Governance and Data Management experience and have worked extensively with a large number of organisations in this area, to enable them to demonstrate compliance with the GDPR and other privacy laws and regulations.

Contact

Michael Daughton
Partner

Head of Risk and Regulatory Consulting
KPMG in Ireland

t: +353 (87) 744 2965
e: michael.daughton@kpmg.ie

Tom Hyland
Director

Data Privacy Lead – Risk and Regulatory Consulting
KPMG in Ireland

t: +353 (87) 050 4223
e: tom.hyland@kpmg.ie

kpmg.ie